Somebody's Listening

. . . and they don't give a damn about personal privacy or commercial confidence. Project 415 is a top-secret new global surveillance system. It can tap into a billion calls a year in the UK alone. Inside Duncan Campbell on how spying entered the 21st century . . .

By Duncan Campbell

***New Statesman*, 12 August, 1988**

They've got it taped

In the booming surveillance industry they spy on whom they wish, when they wish, protected by barriers of secrecy, fortified by billions of pounds worth of high, high technology. **Duncan Campbell** reports from the United States on the secret Anglo-American plan for a global electronic spy system for the 21st century capable of listening in to most of us most of the time

American, British and Allied intelligence agencies are soon to embark on a massive, billion-dollar expansion of their global electronic surveillance system. According to information given recently in secret to the US Congress, the surveillance system will enable the agencies to monitor and analyse civilian communications into the 21st century. Identified for the moment as Project P415, the system will be run by the US National Security Agency (NSA). But the intelligence agencies of many other countries will be closely involved with the new network, including those from Britain, Australia, Germany and Japan--and, surprisingly, the People's Republic of China.

New satellite stations and monitoring centres are to be built around the world, and a chain of new satellites launched, so that NSA and its British counterpart, the Government Communications Headquarters (GCHQ) at Cheltenham, may keep abreast of the burgeoning international telecommunications traffic.
The largest overseas station in the Project P415 network is the US satellite and communications base at Menwith Hill. near Harrogate in Yorkshire. It is run undercover by the NSA and taps into all Britain's main national and international communications networks (*New Statesman*, 7 August 1980). Although high technology stations such as Menwith Hill are primarily intended to monitor international communications, according to US experts their capability can be, and has been, turned inwards on domestic traffic. Menwith Hill, in particular, has been accused by a former employee of gross corruption and the monitoring of domestic calls.

The vast international global eavesdropping network has existed since shortly after the second world war, when the US, Britain, Canada, Australia and New Zealand signed a

secret agreement on signals intelligence, or "sigint". It was anticipated, correctly, that electronic monitoring of communications signals would continue to be the largest and most important form of post-war secret intelligence, as it had been through the war.

Although it is impossible for analysts to listen to all but a small fraction of the billions of telephone calls, and other signals which might contain "significant" information, a network of monitoring stations in Britain and elsewhere is able to tap all international and some domestic communications circuits, and sift out messages which sound interesting. Computers automatically analyse every telex message or data signal, and can also identify calls to, say, a target telephone number in London, no matter from which country they originate.

A secret listening agreement, called UKUSA (UK-USA), assigns parts of the globe to each participating agency. GCHQ at Cheltenham is the co-ordinating centre for Europe, Africa and the Soviet Union (west of the Ural Mountains).

The NSA covers the rest of the Soviet Union and most of the Americas. Australia--where another station in the NSA listening network is located in the outback--co-ordinates the electronic monitoring of the South Pacific, and South East Asia.

With 15,000 staff and a budget of over £500 million a year (even without the planned new Zircon spy satellite), GCHQ is by far the largest part of British intelligence. Successive UK governments have placed high value on its eavesdropping capabilities, whether against Russian military signals or the easier commercial and private civilian targets.

Both the new and existing surveillance systems are highly computerised. They rely on near total interception of international commercial and satellite communications in order to locate the telephone or other messages of target individuals. Last month, a US newspaper, the *Cleveland Plain Dealer*, revealed that the system had been used to target the telephone calls of a US Senator, Strom Thurmond. The fact that Thurmond, a southern Republican and usually a staunch supporter of the Reagan administration, is said to have been a target has raised fears that the NSA has restored domestic, electronic, surveillance programmes. These were originally exposed and criticised during the Watergate investigations, and their closure ordered by President Carter. After talking to the NSA, Thurmond later told the *Plain Dealer* that he did not believe the allegation. But Thurmond, a right-wing Republican, may have been unwilling to rock the boat. Staff members of the Permanent Select Committee on Intelligence said that staff were "digging into it" despite the "stratospheric security classification" of all the systems involved.

The Congressional officials were first told of the Thurmond interception by a former

employee of the Lockheed Space and Missiles Corporation, Margaret Newsham, who now lives in Sunnyvale, California. Newsham had originally given separate testimony and filed a lawsuit concerning corruption and mis-spending on other US government "black" projects. She has worked in the US and Britain for two corporations which manufacture signal intelligence computers, satellites and interception equipment for NSA, Ford Aerospace and Lockheed. Citing a special Executive Order signed by President Reagan. she told me last month that she could not and would not discuss classified information with journalists. But according to Washington sources (and the report in the *Plain Dealer*, she informed a US Congressman that the Thurmond interception took place at Menwith Hill, and that she personally heard the call and was able to pass on details.

Since then, investigators have subpoenaed other witnesses and asked them to provide the complete plans and manuals of the ECHELON system and related projects. The plans and blueprints are said to show that targeting of US **political** figures would not occur by accident. but was designed into the system from the start.

While working at Menwith Hill, Newsham is reported to have said that she was able to listen through earphones to telephone calls being monitored at the base. Other conversations that she heard were in Russian. After leaving Menwith Hill, she continued to have access to full details of Menwith Hill operations from a position as software manager for more than a dozen VAX computers at Menwith which operate the ECHELON system.

Newsham refused last month to discuss classified details of her career, except with cleared Congressional officials. But it has been publicly acknowledged that she worked on a large range of so-called "black" US intelligence programmes, whose funds are concealed inside the costs of other defence projects. She was fired from Lockheed four years ago after complaining about the corruption, and sexual harassment.
Lockheed claimed she had been a pook *[as written]* timekeeper, and has denied her charges of corruption on "black" projects. But the many charges she is reported to have made--such as the use of top secret computers for football pools, or to sell a wide range of merchandise from their offices, and deliberate and massive overcharging and waste by the company--are but small beer in a continuing and wider scandal about defence procurement. Newsham's testimony about overcharging by contractors is now the subject of a major congressional inquiry.

From US sources not connected with Margaret Newsham, we have obtained for the first time a list of the major classified projects in operation at Menwith Hill. The base currently has over 1,200 staff, more than two thirds of them Americans. Other than the ECHELON computer network, the main projects at Menwith Hill are code-named SILKWORTH, MOONPENNY, SIRE, RUNWAY and STEEPLEBUSH. The station also

receives information from a satellite called BIG BIRD.

Project SILKWORTH is, according to signals intelligence specialists, the code-name for long-range radio monitoring from Menwith Hill. MOONPENNY is a system for monitoring satellite communications; RUNWAY is thought to be the **control** network for an eavesdropping satellite called VORTEX, now in orbit over the Soviet Union The base earlier controlled a similar series of satellites called CHALET. The new STEEPLEBUSH **control** centre appears connected with the latest and biggest of the overhead listening satellites. These are code-named MAGNUM, according to US intelligence sources. BIG BIRD, which is not usually connected with Menwith Hill, is a low-orbiting photographic reconnaissance satellite. But investigators have worked out, from details of the clearances necessary to know about BIG BIRD, that this satellite--and indeed, many other satellites, variously disguised as "weather satellites"--also carry listening equipment. One such sigint package is said to have been aboard the doomed space shuttle Challenger, despite its ostensibly civilian purpose.

Recently published US Department of Defense 1989 budget information has confirmed that the Menwith Hill spy base will be the subject of a major $26 million expansion programme. Information given to Congress in February listed details of plans for a four-year expansion of the main operation building and other facilities at Menwith Hill. Although the testimony referred only to a "classified location", the base can be identified because of references to STEEPLEBUSH. According to this testimony, the new STEEPLEBUSH II project will cost $15 million between now and 1993. The expansion is required to avoid overcrowding and "to support expanding classified missions".

During the Watergate affair. it was revealed that NSA, in collaboration with GCHQ, had routinely intercepted the international communications of prominent anti-Vietnam war leaders such as Jane Fonda and Dr Benjamin Spock. Another target was former Black Panther leader Eldridge Cleaver. Then in the late 1970s, it was revealed that President Carter had ordered NSA to stop obtaining "back door" intelligence about US **political** figures through swapping intelligence data with GCHQ Cheltenham.

Among important stations being developed in the new P415 network, sources indicated, are Bude in Cornwall, mainly run by GCHQ, Bad Aibling in Germany, and two sites in the People's Republic of China (which are used only for monitoring the USSR). The western intelligence agencies have not yet resolved the question of how to replace the recently upgraded British intelligence listening station at Chung Hom Kok in Hong Kong (which at the moment listens to China itself) when the colony is handed back to China next decade.

In Australia three months ago, New Zealand Defence Minister Bob Tizard revealed that two Australasian interception stations planned for the early 1990s will be targeted on

new communications satellites launched by third world countries such as India and Indonesia. The new satellite spy bases are at Geraldton in northern Australia and Blenheim, New Zealand. The similar British spy base at Morwenstow, near Bude, Cornwall, has been continuously expanded throughout the 1980s, including the provision of massive US analysis computers.

If Margaret Newsham's testimony is confirmed by the ongoing Congressional investigation, then the NSA has been behaving illegally under US law--unless it can prove either that Thurmond's call was intercepted completely accidentally, or that the highly patriotic Senator is actually a foreign spy or terrorist. Moreover NSA's international phone tapping operations from Menwith Hill and at Morwenstow, Cornwall, can only be legal in Britain if special warrants have been issued by the Secretary of State to specify that American intelligence agents are persons to whom information from intercepts must or should be given. This can not be established, since the government has always refused to publish any details of the targets or recipients of specific interception warrants.

When the Menwith Hill base was first set up there was no British law controlling phone tapping, or making unauthorised interception (such as by foreign intelligence agencies) illegal. Now there is, and telecommunications interception by the Americans from British territory would clearly be illegal without the appropriate warrant.

When the new Interception of Communications Act was passed in 1985, however, it was obviously designed to make special provision for operations like ECHELON or Project P415 to trawl all international communications to and from Britain. A special section of the Act, Section 3(2), allows warrants to be issued to intercept any general type of international messages to or from Britain if this is "in the interests of national security" or "for the purpose of safeguarding the economic well-being of the United Kingdom". Such warrants also allow GCHQ to tap any or all other communications on the same cables or satellites that may have to be picked up in order to select out the messages they want. So whether or not a British government warrant can legally allow American agents to intercept private British communications, there is no doubt that British law as well as British bases have been designed to encourage rather than inhibit the booming industry in international telecommunications surveillance.

Both British and American domestic communications are also being targeted and intercepted by the ECHELON network, the US investigators have been told. The agencies are alleged to have collaborated not only on targeting and interception, but also on the monitoring of domestic UK communications.

Special teams from GCHQ Cheltenham have been flown in secretly in the last few years to a computer centre in Silicon Valley near San Francisco for training on the special

computer systems that carry out both domestic and international interception.

The centre near San Francisco has also been used to train staff from the "Technical Department" of the People's Liberation Army General Staff, which is the Chinese version of GCHQ. The Department operates two ultra-secret joint US-Chinese listening stations in the Xinjiang Uighur Autonomous Region, close to the Soviet Siberian border. Allegedly, such surveillance systems are only used to target Soviet or Warsaw Pact communications signals, and those suspected of involvement in espionage and terrorism. But those involved in ECHELON have stressed to Congress that there are no formal controls over who may be targeted. And I have been told that junior intelligence staff can feed target names into the system at all levels, without any check on their authority to do so.

Witnesses giving evidence to the Congressional inquiry have discussed whether the Democratic presidential contender Jesse Jackson was targeted; one source implied that he had been. Even test engineers from manufacturing companies are able to listen in on private citizens' communications, the inquiry was told.

But because of the special Executive Order signed by President Reagan, US intelligence operatives who know about such politically sensitive operations face jail sentences if they speak out--despite the constitutional American protection of freedom of speech and of the press. And in Britain, as we know, the government is in the process of tightening the Official Secrets Act to make the publication of any information from intelligence officials automatically a crime, even if the information had already been published, or had appeared overseas first.

Note: **Duncan Campbell** has generously provided additional US sources of information on electronic inteception which shall be offered on this site when available.

Selected references:

1972 Winslow Peck, former NSA analyst, *Ramparts* interview on NSA electronic interception: http://jya.com/nsa-elint.htm (89K)

1976 **Duncan Campbell**, "British MP Accuses U.S. of Electronic spying," *New Scientist*, August 5, 1976, p. 268.

1979 **Duncan Campbell**, "The Threat of the Electronic Spies," *New Statesman*, February 2, 1979, pp. 140-44.

1980 **Duncan Campbell**, "Society Under Surveillance," *Policing The Police,* Vol.

2. (Ed: Ha.) John Calder, London.

1980 **Duncan Campbell** and Clive Thomas, "BBC's Trade Secrets," *New Statesman*, July 4, 1980, pp. 13-14.

1980 **Duncan Campbell** and Linda Melvern, "America's Big Ear on Europe," *New Statesman,* July 18, 1980, pp. 10-14.

1981 **Duncan Campbell**, (Ed.) "Big Brother Is Listening - Phone tappers and the security state", 1st ed. Vol. 2. *New Statesman*, London.

1983 **Duncan Campbell**, "Spy in the Sky," *New Statesman,* September 9, 1983, pp. 8-9.

1983 James Bamford, *The Puzzle Palace: A Report on America's Most Secret Agency,* London, Penguin. Excerpts:

Chapter 8 - Partners (76K)

Chapter 9 - Competition (69K)

Chapter 10 - Abyss (43K)

1984 **Duncan Campbell**, *The Unsinkable Aircraft Carrier: American Military Power in Britain*, London, Michael Joseph.

1985 Jeffrey T. Richelson and Desmond Ball, *The Ties That Bind: Intelligence Cooperation Between the UKUSA Countries,* London, Allen & Unwin.

1986 **Duncan Campbell** and Patrick Forbes, "UK's Listening Link to Apartheid," *New Statesman*, August 1, 1986, pp. 101-11.

1986 **Duncan Campbell** and S. Connor, *On The Record*, Michael Joseph, London.

1987 William Burrows, *Deep Black: Space Espionage and National Security*, New York, Random House. Excerpt:

Chapter 8 - Foreign Bases: A Net Spread Wide (71K)

1989 Jeffrey T. Richelson, *The U.S. Intelligence Community*, New York, Ballinger.

Excerpts:
Chapter 8 - Signals Intelligence (97K)

Chaper 12 - Exchange and Liaison Arrangements (72K)

1996 Nicky Hager, *Secret Power*: *New Zealand's Role In the International Spy Network*, Craig Potton, Nelson, New Zealand.

1996 *Intelligence Online* report on UKUSA cooperation:
http://www.blythe.org/Intelligence/readme/brits-usa.int45

1997 *Daily Telegraph* report "Spies Like US" on Mentwith Hill (with aerial photo) and other commentary:
http://www.accessone.com/%7Erivero/POLITICS/ECHELON/echelon.html

1998 Nicky Hager, *Covert Action Quarterly* article on ECHELON:
http://jya.com/echelon.htm (30K)

1998 European Parliament, STOA report, *Assessment of the Technologies of*

Political Control: http://jya.com/stoa-atpc.htm (295K)
The book excerpts provide extensive additional sources.

The National Security Agency Web site: http://www.nsa.gov:8080

Related US Office of Technology Assessment reports on electronic surveillance, 1972-1996: http://jya.com/esnoop.htm